UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,452	01/05/2001	Scott C. Harris	FILE-DOMAIN/SCH	5147

23844 7590 08/09/2006

SCOTT C HARRIS
P O BOX 927649
SAN DIEGO, CA 92192

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/755,452	HARRIS, SCOTT C.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-10,12-16,18-23,25 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-10, 12-16, 18-23, 25, and 26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication amendment filed on 18 April 2006, with original application filed 05 January 2001, and acknowledgement of continuing data filing date of 21 July 2000.

2. Claims 1, 3-10, 12-16, 18-23, 25, and 26 are currently pending in this application. Claims 1, 10, 14, 22, and 23 are independent claims. Claims 1, 9, 10, 14, 20, 22, 23, 25, and 26, have been amended. Claims 2, 11, 17, 24, and 27 have been cancelled.

Claim Objections

3. Claims 3 and 4 are objected to because of the following informalities: both claims depend from claim 2, which has been cancelled by amendment. Appropriate correction is required. For examining purposes it is assumed claims 3 and 4 depend from claim 1.

4. Claim 10 is objected to because of the following informalities: "prestored critera" is misspelled. Appropriate correction is required.

Abstract Objection

5. Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

Examiner notes: an abstract submission is limited to 150 words, the applicant's submitted abstract has only 25 words and lacks details to quickly determine the improvement being claimed.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 3-10, 12-16, 18-23, 25, and 26 have been considered but they are moot due to new grounds of rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1, 4, 10, 12, 14-16, 18, 20, 21, and 23,** are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al. U.S. Patent No. 6,820,063 (hereinafter '063).

As to independent claim 1, "A method, comprising: identifying a user using unique information" is taught in '063 col. 17, lines 42-44;

"encrypting a first plurality files a computer using a first encryption key that is associated with said user" is shown in '063 col. 17, lines 42-55 (note the 'first encryption key is interpreted to be equivalent to the 'storage key';

"responsive to said identifying, using a program and a first decryption key, corresponding to said first encryption key, to allow changes to be made to any of said first plurality of files associated said user" is disclosed in '063 col. 17,
lines 53-64 (note: accessing data in combination with the application is interpreted to be equivalent to allow user to make changes);
the following is not explicitly taught in '063:

"allowing reading of said first plurality of files using a second, recovery decryption key, different than said first decryption key, and which is intended for recovery of files when said first decryption key becomes unavailable" however '063 teaches "When the ephemeral key expires, the DRMOS developer issues replacement components. As with the two-section boot block shown in FIG. 7B, the master private key is only used to sign the certificates for the ephemeral keys so it is less likely to be compromised. Because the ephemeral keys are valid for only a short duration, public release of a private ephemeral key has limited impact", in col. 15, lines 23- 29; note it is obvious the DRMOS will issue replacement components, i.e. keys if the a recovery decryption key is needed because the first key becomes unavailable, i.e. 'compromised' or 'expires'.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 digital right for content downloaded to a subscriber computer to include a means to issue recovery decryption key if first decryption key becomes unavailable.

One of ordinary skill in the art would have been motivated to perform such a modification in order to protect content stored on computers. As indicated by '063 (see col. 14, lines 51 et seq.) "If the DRMOS developer's private key used to sign the boot block is compromised, the key pair must be changed and thus all boot blocks must be reissued to subscriber computers. FIG. 7B illustrates an alternate embodiment of a boot block that ameliorates this problem. Boot block 710 comprises a basic boot section 711 and an intermediate boot section 713. The basic boot section 711 contains boot code 715 that validates and loads the intermediate boot section 713 and components not provided by the DRMOS developer. The intermediate boot section 713 contains boot code 717 that validates and loads components from the DRMOS developer. The intermediate boot section 713 is signed with a special boot block private key. The basic boot code 715 uses a corresponding boot block public key 719 stored in the basic boot section 711 to validate the intermediate boot section 713. Components 727 from the DRMOS developer are signed 729 with the developer's standard private key and the intermediate boot section 713 uses the DRMOS developer's standard public key 721 to validate those components".

As to dependent claim 4, "wherein said unique information includes a unique number indicative of hardware in the computer system" is taught in '063 col. 11, line 46 through col. 12, line 36.

As to independent claim 10, "A method, comprising: defining an operating system that operates based on stored operating system files" is taught in '063 col. 11, lines 23-30;

"detecting an update requested for at least one of said operating system files" is shown in '063 col. 13, lines 3-19;

"checking a digital certificate associated with the update" as well as **"and allowing the update to be conducted only if the digital certificate matches a pre-stored criteria"** is disclosed in '063 col. 11, lines 23-51;

the following is not explicitly taught in '063:

"**said checking being carried out over the Internet"** however '063 indicates that "Furthermore, not all versions of a component may be trusted. Because the rights manager certificate contains the version number of the component, it can be used to verify the trust level of a particular version. One embodiment of the loading process checks a component certification revocation list (CRL) to determine whether a component signature has been revoked. The CRL can be provided by the content provider or the DRMOS developer. An exemplary embodiment of a CRL is illustrated in FIG. 4. Each entry 401 contains the name of the component 403, the version 405, and the signer 407 whose signature is revoked. The particular CRL used becomes part of the operating system identity using a standard hashing function described further below" in col. 12, lines 7-20, note to check the CRL the computer would have to communicate over a WAN or Internet as indicated in col. 6, lines 42-57.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 digital right for content downloaded to a subscriber computer to include a means check certificates over the Internet. One of ordinary skill in the art would have been motivated to perform such a modification to have updated information. As indicated by '063 (see col. 12, lines 21 et seq.) "Alternatively, if the rights manager certificates on the components are short-lived and must be renewed periodically, then a version that is found to be untrustworthy will not have its certificate renewed. This alternate embodiment requires a secure

time source to be available on the subscriber computer ... A monotonic counter in the CPU can serve as this secure time source since it only counts up and cannot be reset "back in time." For example, a monotonic counter that is periodically incremented while the CPU is active, and that cannot be reset, can be used in conjunction with a secure time service, such as a secure Internet time service".

As to dependent claim 12, "further comprising forming encrypted files by requiring a unique information, and using said unique as part of an encryption and/or decryption operation" is taught in '063 col. 16, lines 33-60.

As to independent claim 14, "A computer, comprising: a processor; a file accessing element, controlled by a controlling operation, said file accessing part encrypts certain files in the computer in a way that prevents access specified files but allows access to other files unless first file decryption information is used to allow access to first encrypted files; and" is shown in '063 col. 10, lines 1-25;

the following is not explicitly taught in '063:

"and wherein said file accessing part also allow access to said specified files using second file decryption information, different than said first file decryption information, where said second file decryption information is a recovery key intended for recovering said specified files if said first file decryption information is unavailable" however '063 teaches "When the ephemeral key expires, the DRMOS developer issues replacement components. As with the two-section boot block shown in FIG. 7B, the master private key is only used to sign the certificates for the ephemeral keys so it is less likely to be compromised. Because the ephemeral keys are valid for only a short duration, public release of a private

ephemeral key has limited impact", col. 15, lines 23-29; note it is obvious the DRMOS will issue replacement components, i.e. keys if the a recovery decryption key is needed because the first key becomes unavailable, i.e. 'compromised' or 'expires'.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 digital right for content downloaded to a subscriber computer to include a means to issue recovery decryption key if first decryption key becomes unavailable. One of ordinary skill in the art would have been motivated to perform such a modification in order to protect content stored on computers. As indicated by '063 (see col. 14, lines 51 et seq.) "If the DRMOS developer's private key used to sign the boot block is compromised, the key pair must be changed and thus all boot blocks must be reissued to subscriber computers. FIG. 7B illustrates an alternate embodiment of a boot block that ameliorates this problem".

As to dependent claim 15, "wherein said file accessing element allows access to all read files, and prevents access to read/write files without said unique information" is disclosed in '063 col. 17, lines 43-55.

As to dependent claim 16, "wherein said file accessing element allows access to certain read write files which are designated as being special, is shown in '063 col. 17, lines 56-64.

As to dependent claim 18, "wherein said encrypting comprises obtaining personal information from a user, and using said personal information to form encryption and/or decryption operations" is taught in '063 col. 17, lines 42-64.

As to dependent claim 20, "further comprising file storage part which includes removable memory and wherein unencrypted read/write access is allowed to said

removable memory" is shown in '063 col. 10 lines 1-10 (note it is understood the derivative of making unencrypted copies is part of a license agreement).

As to dependent claim 21, "wherein said file accessing element is part of an operating system" is taught in '063 col. 8, lines 41-50.

As to independent claim 23, "A method, comprising: obtaining an encryption and decryption code associated with a user of the computer system determining specified files on the computer system having been designated as being encrypted; and encrypting said specified files said computer system, using an encryption key that can be decrypted using either said decryption code for said user" is disclosed in '063 col. 17, lines 42-64
the following is not explicitly taught in '063:

"or with a second, recovery decryption key, different than said first decryption key and which intended for recovery of files when said first decryption key becomes unavailable" however '063 teaches "When the ephemeral key expires, the DRMOS developer issues replacement components. As with the two-section boot block shown in FIG. 7B, the master private key is only used to sign the certificates for the ephemeral keys so it is less likely to be compromised. Because the ephemeral keys are valid for only a short duration, public release of a private ephemeral key has limited impact", in col. 15, lines 23- 29; note it is obvious the DRMOS will issue replacement components, i.e. keys if the a recovery decryption key is needed because the first key becomes unavailable, i.e. 'compromised' or 'expires'.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 digital right for content downloaded to a subscriber computer to include a means to issue recovery decryption key if first decryption key becomes unavailable.

One of ordinary skill in the art would have been motivated to perform such a modification in order to protect content stored on computers. As indicated by '063 (see col. 14, lines 51 et seq.) "If the DRMOS developer's private key used to sign the boot block is compromised, the key pair must be changed and thus all boot blocks must be reissued to subscriber computers. FIG. 7B illustrates an alternate embodiment of a boot block that ameliorates this problem".

9. **Claims 13, 22, 25, and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over '063 in further view of Tello U.S. Patent No. 6,463,537 (hereinafter '537).

As to independent claim 22, "A method comprising: identifying a first user; using an operating system associated program computer designate a first plurality of files a computer, as being associated with said first user and to encrypt said plurality of files using a first encryption key associated with said first user" is shown in '063 col. 17, lines 42-55;

" and to prevent reading contents said first plurality of read/write files when said first user not identified" is disclosed in '063 col. 17, lines 56-64;

the following is not explicitly taught in '063:

"identifying a second user; using an operating system associated program computer designate a second plurality of files a computer, as being associated with said second user and to encrypt said plurality of files using a second encryption key associated with said second user and to prevent reading contents said second plurality of read/write files when said second user not identified" however '063 discloses in col. 17, lines 56-64 that the files are assigned to a unique user, therefore it is obvious the assignment of keys is to multiple users or subscribers, i.e. second users;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 digital right for content downloaded to a subscriber computer to include a means to issue encryption and decryption keys to a second user. One of ordinary skill in the art would have been motivated to perform such a modification in order to protect content stored on computers. As indicated by '063 (see col. 16, lines 33 et seq.) "In order to protect content permanently stored on the subscriber computer, the DRMOS must provide a secure storage space. In essence, the DRMOS must securely store private keys or session keys for use with encrypted content, or provide some other mechanism for keeping these keys secret from other OSs or system level software. These keys can be used for the secure storage and retrieval of protected information. In the exemplary embodiments described in this section, the information to be stored in a protected format is encrypted using one of a set of keys that may be generated by a function 800 (FIG. 8) provided by the CPU. The storage key generation process is tightly coupled to the DRMOS so that the same key cannot be generated by the CPU for an unrelated operating system, or by any software on another computer. Three types of storage keys are envisioned as illustrated in FIG. 8: an OS storage key 801, an application storage key 811, and a user storage key 821. Each key is specific to the entity that requests it".
the following is not taught in '063:

"allowing other unencrypted files on said system be to be read when said first and second user is not identified, but preventing writing to said other unencrypted files; and establishing special files on said system which are unencrypted but which can be written to and read by the system only after security operation and establishing special files on said system which are unencrypted but which can be written to and read by the system only

after specified security operation" however '537 teaches "Modifications to the DDL and the inclusion of an I/O address map and circular memory buffer circuits also permit this invention to encrypt or decrypt selected data" in col. 19, lines 55-58. Note '063 teaches three methods of restricting access to data on a computer by OS, application, and user; therefore it is inherent in '063 that a first and second user could access information utilizing an authorized OS. Reference '537 teaches that certain file parts can be stored encrypted or unencrypted.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 a rights management system for digital content to include a means utilize encryption mechanisms to protect selected files. One of ordinary skill in the art would have been motivated to perform such a modification to because as the use of computers increases the need to protect the information on the computers grows. As indicated by '537 (see col. 1, lines 24 et seq.) "As the prevalence and importance of computers grows and their portability increases, so too does the need to protect these systems and the data stored within them from unauthorized access and theft".

As to dependent claim 13, "and carrying out least one security measure said special files" is taught in '063 col. 8, line 63 through col. 9, line 14;

the following is not taught in '063: **"further comprising establishing special files which are read/write files that are not encrypted"** however '537 teaches "Modifications to the DDL and the inclusion of an I/O address map and circular memory buffer circuits also permit this invention to encrypt or decrypt selected data" in col. 19, lines 55-58.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 a rights management system for digital content to include a

means utilize encryption mechanisms to protect selected files. One of ordinary skill in the art would have been motivated to perform such a modification to because as the use of computers increases the need to protect the information on the computers grows. As indicated by '537 (see col. 1, lines 24 et seq.) "As the prevalence and importance of computers grows and their portability increases, so too does the need to protect these systems and the data stored within them from unauthorized access and theft".

As to dependent claim 25, "wherein said unique code a code from a smart card" is taught in '537 col. 5, lines 25-27 "holder of a particular smart card".

As to dependent claim 26, "wherein said unique code a code from a biometric" is shown in '537 col. 7, lines 53-57 "This allows for the addition of devices such as a biometric reader"

10. **Claims 3, 5-7, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over '063 in view of Orita U.S. Patent No. 5,163,147 (hereinafter '147).

As to dependent claim 3, the following is not specifically taught in '063: **"wherein said unique information includes a user password"** however '147 teaches "The user inputs ID information (incl. a password)" in col. 3, line 10.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 digital right for content downloaded to a subscriber computer to include a means wherein unique information includes a user password. One of ordinary skill in the art would have been motivated to perform such a modification because passwords are a known means of user authentication. As indicated by '147 (see col. 1, lines 18 et seq.) "Such a security system includes a system which is known in the art or can be easily devised and in

which a user list is set for each file to be protected so as to inhibit the file access even if a user other than the listed users makes an access request for the file. Further, a system is provided in which a file list for permitting access to the file for each user is set and a file access is inhibited when a file other than the listed files is accessed by a corresponding user. In addition a system is provided in which a pass word is previously set and only a user who inputs the pass word via the terminal device is permitted to access the file".

As to dependent claim 5, "further comprising designating a second plurality of files on the computer as read only" and **"but not allowing any changes to said read only files"** is shown in '147 col. 5, lines 1-7;

"and storing unencrypted information in said read files" is disclosed in '063 col. 10, lines 1-48 (Note: the DRMOS determines the "license" with the files and what derivative use can be made of the content).

As to dependent claim 6, "further comprising establishing a plurality of special files within said plurality of files, said special files being" and **"and establishing special security measures for said special files"** is taught in '147 col. 3, lines 1-21 "The read/write memory 14 includes an area 14a for storing operator profile (OP) information ... Access protection information 12a (not shown) is included in each of the user programs 12e and each of the user files";

"said special files being unencrypted read/write files" is disclosed in '063 col. 10, lines 1-48 (Note: the DRMOS determines the "license" with the files and what derivative use can be made of the content).

As to dependent claim 7, "wherein said security measures include determining whether a specified program actually accessing the file, and only allowing file access by said specified program" is disclosed in '147 col. 4, lines 49-60 "When an access request for a user file in the storage unit 12 is made by the user program (setp S11), permission of execution of the file access is verified" as well as '063 col. 10, lines 1-3.

As to dependent claim 19, "wherein said unique information includes a user password" is taught in '147 col. 3, line 10.

11. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over '063 in further view of Porter et al. U.S. Patent No. 6,675,299 (hereinafter '299).

As to dependent claim 8, the following is not taught in '147: **"further comprising of accesses based on specified detecting certain kinds security criteria, and maintaining a log of said accesses including information about a program that made said accesses"** however '299 teaches "Finally, the document profile 710 contains the access history of the document. Access history includes information defining the user who created the document, and all users who accessed, modified, printed, or otherwise had contact with the document. The access history information includes the name of the user, the type of action performed by the user, and the time the user accessed the document" in '299 col. 8, lines 32-39.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 a method for controlling access to files based on user access level to include a management system, which maintains a history of file use. One of ordinary skill in the art would have been motivated to perform such a modification to because a management system is needed that maintains a log of access rights with an association to files.

As indicated by '299 (see col. 2, lines 6-17.) "This two-step log-in procedure creates problems when the access rights are changed or when, for example, new users must be added to both security systems. Multiple sets of security information create configuration control and consistency problems ... Therefore, it is apparent that a need exists for a document management system which does not use a separate database and which does not utilize multiple security systems".

12. **Claim 9,** is rejected under 35 U.S.C. 103(a) as being unpatentable over '063 in further view of Prihoda et al. U.S. Patent No. 6,789,195 (hereinafter '195).

As to dependent claim 9, the following is not taught in '063: **"further comprising selecting a first file, and designating said file as being encrypted, to change an encryption status of said first file"** however '195 teaches "it provides for this to be done exclusively at the user end. In this case, the data are available in unencrypted form only at the doctor's end (that is to say at the client), and the data are encrypted at the doctor's end even before they are transmitted to the central database (server). This makes attacks on the central data storage point, which is at risk, very difficult, in particular even attacks by the system administration. Thus, in the method according to the invention, only encrypted data, or only encrypted data parts which contain critical information and, as a consequence, need to be especially protected, are transmitted via the communications link, which can be tapped. Non-critical data may also be transmitted, of course, in unencrypted form. Protection against unauthorized data access is furthermore ensured in that a special key is required for encryption and/or decryption, which key is allocated exclusively to authorized users from a central further database. This key is thus passed only to the users who are authorized for access, for example only to doctors who are

authorized for access. The data may be composed of data parts and association data which identify a person or an object and describe a person or an object, in which case the identifying data parts are stored in a first database and the descriptive data parts are stored in a second database, in each case with an association data item. Those data parts which are stored in the other database can be found using the identically formed association data, and in which case at least the association data item of the identifying data parts and, if required, the descriptive data parts are encrypted, and can be decrypted using the transmitted key. Two separate databases are thus used in this case and preferably, but not necessarily, do not communicate with one another. The databases are object-oriented databases which, for example, contain patient data in the form of patient-specific files. At least the critical data are encrypted, non-critical data need not necessarily be stored in encrypted form in the second database" in col. 2, lines 3-61.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '063 a method for controlling access to files based on user access level to include a means to change the encryption status of a file. One of ordinary skill in the art would have been motivated to perform such a modification to because data stored is composed of critical and non-critical parts. As indicated by '195 (see col. 1, lines 14 et seq.) "Data to be stored in a database are ever more frequently composed of non-critical parts, whose contents require no special secrecy, and critical data which, if at all, may be accessed only by a limited range of users. In order to store such critical data with protected access, it is known for the data to be stored in encrypted form. Cryptographic methods (for example DES, RAS, IDEA) are used for this purpose, and use symmetrical or asymmetrical keys in order to encrypt the data. In known methods for secure communication, the data are encrypted while being transmitted (line

encryption) between the client and the server, the data then exist in unencrypted form once again at the central point, and are generally stored in unencrypted form in a central database. With these methods, there is a security gap, since anyone who has administrative access to the central database can read all the data".

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Slivka et al. U.S. Patent No. 6,049,691

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
3 August 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100